	Georgia Technology Authority	
Title:	**Authorization and Access Management**	
PSG Number:	SS-08-010.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 3
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Agencies must limit access to state facilities and information resources and manage access once granted.	

PURPOSE

Lack of managed access controls to sensitive or proprietary state information assets can result in unauthorized or inadvertent disclosure, modification or deletion of the information asset or render it unavailable. Access Control measures are needed to ensure that even legitimate users have access to only that information for which they are authorized and need to perform their official duties. This standard establishes minimum access control requirements.

SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (Policy)

STANDARD

Agencies that create, use or maintain information assets of the State of Georgia shall implement access control measures that restrict physical and logical access to information, information systems and facilities to only authorized individuals, except where specifically designated as public access resources.

Access to state information resources, not designated for general public use, shall require a formal process of identity and access management to include positive user identification, explicit Data Owner approval, user provisioning, and system authentication.

Agency Head, Data Owner or their designee shall establish and document access authorization and control policies and procedures.

System Owners shall issue and manage access credentials in accordance with established Data Owner policy and procedures.

Access rights shall be granted based on the principle of least privilege, need-to-know, specific business needs and job function.

Access granted to third-parties requires a signed contract.

Access privileges shall be terminated or modified promptly upon change in duties, employment status or extended periods of inactivity.

Privileged (super user, sys admin and/or system/service accounts for auto processing) access activities on systems categorized as moderate or high shall be audited. Misuse of privilege access shall be reported in accordance with established agency incident response and reporting procedures.

Default access privileges shall be set to “deny all” or “no access”

Information Security Officers shall conduct periodic reviews to validate the appropriateness of user accounts and access privileges.

GUIDELINES

Internal access control standards and procedures should be established and maintained by the Data Owner. They should clearly define the authorization process for granting access to the information assets. They should be based on business needs and security requirements.

Where systems are providing access to State of Georgia resources to the general public, the information designated as public should be segregated from all non-public resources in specially designated public domain resource configurations.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Access Control (Policy)
- Password Authentication (Policy)
- Third-Party Access (Policy)
- Network Access-Session Controls (Standard)
- Information Security Management Organization (Standard)

REFERENCES

- Georgia Open Records Act (50-18-70 et seq)
- Georgia Computer Crimes Act (16-9-93 et seq)

TERMS and DEFINITIONS

Access Control is the set of rules and deployment mechanisms that enables or restricts physical and logical access to information systems.

Physical Access is the ability to enter areas or facilities where information systems and technology assets reside.

Logical Access is the ability to read, write or, execute records or data contained in the information system.

Identity and Access Management is a set of processes and supporting infrastructure for creating, maintaining, and using digital identities in accordance with business policies and needs.

Authorization is the formal approval, granted by Data Owner, for an individual to gain access to a facility, system, or other non-public information asset.

Data/Information Owner is a business person whom defines the controls necessary to protect the data within their business function accepts the risks associated with operating an information system processing that data.

Positive User Identification is the validation of user requesting and being granted access credentials to non-public state information resources.

Access Privileges or Rights refers to powers granted to a system user that defines the levels of access they have to read, write, or execute data or system resources.

Need-to-Know is a confidentiality principle that says access should be denied even if an individual has all the necessary official approvals to access certain information but does not need access to the specific information to conduct of one's official duties

Principle of Least Privilege refers to assigning access rights that provide the most restrictive access or provides no more access to systems or information than is necessary to perform one's official duties.

Note: PSG number administratively changed from S-08-010.01 on September 1, 2008.